

5 March 2008

## Standardised Chip & Pin terminologies and educational messages

### 1. Introduction

At The Banking Association South Africa's Payment Strategy Steering Committee meeting on 29 August 2007, it was agreed that the Payment Strategy Department of The Banking Association (PayStrat) should compile a document proposing standardised Chip & Pin terminology and core messages that could be used by the Industry in their individual merchant and customer training and marketing initiatives. The content is intended to be high level and general in nature. The benefit of such a standardised approach is that a consistent message will be communicated to the cardholder and merchant preventing possible confusion. It remains the responsibility of individual banks to train their merchants and to properly inform their cardholders on the detail of their specific agreements and arrangements. **NOTE: This document serves as a suggested best practice document to be used by banks on a voluntary basis.**

### 2. Background

As a result of banks starting to issue Chip & Pin cards, it is important that all Chip & Pin terminologies and messages agreed to date should be applied consistently across the Industry. This document provides a summary of previously agreed (by the EMV Forum) terminologies and messages that should ideally be used by the Industry, supported by messages used in the United Kingdom at the launch of their Chip & Pin initiative. It is proposed that the information contained in this document be used by the Industry as a point of reference when formulating individual merchant and customer training and marketing initiatives. It is proposed that training material should clearly indicate what information pertains to the merchant and what to cardholders.

### 3. Terminology

#### 3.1 Core Terminology

When referring to EMV enabled cards, the words "Chip & PIN" should be used in stead of terms such as EMV or Smart card.

#### 3.2 Additional Terminology

This has been included as Annexure A.

In addition a Core Message and Awareness presentation aimed at merchant staff (Ref 37815) has been provided for assistance.

### 4. Account holders

#### 4.1 Key message

The way that we pay for goods and services with credit and debit cards, is changing. In order to make card payments in South Africa more secure, Chip &

Pin cards are currently in the process of being deployed. These cards require customers to key in a unique PIN when making a payment, instead of signing a receipt. This is similar to keying in a PIN when using an ATM or a debit card at Point of Sale. Some terminals or cards may require both signature and PIN.

#### 4.2 Frequently asked questions for cardholders:

A number of frequently asked account holder questions with proposed answers are provided below:

##### 4.2.1 *Why am I getting a new Chip & Pin card?*

Chip & Pin cards introduce a much more secure way to use debit and credit cards. If the Chip & Pin card is lost or stolen, the chip's risk management system blocks the card. For South African cards this occurs after the third attempt to enter the PIN incorrectly. A Chip & Pin card also has data storage capabilities far beyond the magnetic stripe. Chip & Pin cards will be able to support new or enhanced products and services.

##### 4.2.2 *Must I use a PIN, as I prefer to use a signature to authorise my transactions?*

Using a PIN means that only you as the authorised Cardholder can make purchases with your card. Eventually this system will be introduced across the global market to all Cardholders and retailers on a phased basis to improve security. If you find it difficult to remember your PIN, you may be able to change it to a more memorable number, but your signature based card is still valid until you are otherwise notified.

##### 4.2.3 *What happens if I key in the wrong PIN?*

Do not worry if you key in the wrong number - you have three chances to get it right (for a South African card). If you enter the wrong number three times in a row, your card will be 'blocked'. This stops anyone other than you from using your card and having more chances to guess your PIN. The screen on the PIN pad will tell you if you entered a wrong PIN number. If your card is blocked, please contact your bank who will tell you how to unblock your card.

##### 4.2.4 *Will my new Chip & Pin card still need to be signed on the reverse?*

Yes, as all shops have not yet switched to Chip & Pin applications on their point of sale terminals, you will be required to sign the customer receipt at such shops as is currently the case. In addition, the card will continue to be swiped at the point of sale terminal and will not be inserted.

##### 4.2.5 *Will I be able to use a Chip & Pin card overseas?*

You will still be able to use your cards overseas as you do today. The international card schemes will ensure that SA Cardholders can use their cards at overseas retailers and ATMs as they do at present. The long-term global objective is for all countries to use Chip & Pin as the common method of Cardholder identification.

## 5. **Merchants**

### 5.1 Key message

The way that cardholder customers pay for goods and services with credit and debit cards is changing. In order to make card payments in South Africa more secure, Chip & Pin cards are currently in the process of being deployed. These

cards require customers to key in a unique PIN when making a payment, instead of signing a receipt. This is similar to keying in a PIN when using an ATM or when doing a debit card transaction. It does not replace current signature based cards at the moment.

## 5.2 Frequently asked questions for Merchants

A number of frequently asked Merchant staff questions with proposed answers are provided below.

### 5.2.1 *How do I know when a customer has a Chip & Pin card?*

Chip & Pin cards have the chip (a small metal-coated area) on the top left corner on the front of the card. This means that the chip must be inserted and not swiped.

### 5.2.2 *Do customers require a PIN for all their Chip & Pin card purchases, i.e. debit and credit cards?*

Yes, they do.

### 5.2.3 *How does the payment process work for Chip & Pin cards?*

For any card with a chip, follow the prompts on the terminal screen. The terminal will tell you what to do, whether to ask for a PIN or to continue asking for a signature. The card will still be signed on the back.

Whilst cards are being replaced, there will be some cards that have Chip but will still ask for signatures. If the terminal prompts you to ask for a signature, do not worry, this is correct. Just follow the prompts.

### 5.2.4 *Who should key in the PIN?*

Customers must always enter their own PIN. The terminal will prompt for the customer to enter the PIN. If they want you to do it for them, you must explain that this is not secure and show them how to enter the PIN themselves.

PINs are secret numbers and should remain so! The new PIN pads typically have in-built privacy shields to ensure this. If you have a PIN pad with a flexible wire, pass the PIN pad to the customer so they can hold and shield it with their body. You can help as well by being discreet and not looking at customers when they key in their PIN. Never let a customer tell you their PIN – even if they want to.

If a customer feels that someone may have seen him/her entering his/her PIN, you should advise him/her to change his/her PIN, which she/he can do by going to his/her Bank.

### 5.2.5 *What should I do if a customer has forgotten or does not know his/her PIN?*

In the early stages of your Chip & Pin rollout, you may find that customers do not remember their PINs. Different approaches are required for different cards, depending on the issuing bank (card issuer). Once you have inserted the card in the terminal and you get to the point where a PIN is requested, should the customer indicate that they do not remember their PIN, follow the prompts on the terminal. Some banks' cards will prompt a decline response by the terminal, whilst other cards will allow the processing of the transaction via signature and/ or the magnetic stripe.

Where the card prompts a decline response, the best advice is to ask the cardholder to contact his card issuer or go to his issuing bank's nearest branch to have the PIN reset.

The sooner customers use the new system, the better - avoid any request to override the PIN entry unless authorised by your supervisor and only in the cases where it is in fact possible. If the customer says they can not remember their PIN, pay particular attention to the card and signature checks - in case the reason that they do not know the PIN, is that the card is stolen.

#### 5.2.6 *How do I know that the PIN is blocked?*

As the card is inserted in the POS device, if a PIN is blocked, the terminal will decline the transaction immediately. Depending on the terminal type, one of the following messages could be displayed, "PIN limit exceeded", "Limit Exceeded" or simply "Transaction declined, please contact issuer". This usually means that a customer has entered the wrong PIN three times in a row (for a South African card) and the card has been made temporarily unusable. For foreign cards, the amount of attempts at a PIN may differ. The terminal prompt will tell you whether payment on this card can be made using signature or whether the customer needs to give you a different method of payment.

You should advise customers to call their bank who will tell them how to unblock the PIN.

#### 5.2.7 *Declined transactions – what to do?*

Transactions will be declined when the customer has entered the wrong PIN three times consecutively. In addition, transactions will continue to be declined for the same reasons as before.

#### 5.2.8 *Refunds*

The cardholder must be on site for a refund. If a purchase has been verified by PIN, this will usually be indicated on the receipt. Due to the different rules for different card types and banks, a PIN may or may not be requested by the terminal to complete the transaction. .

#### 5.2.9 *Accepting magnetic stripe cards*

Some cardholders, especially those from other countries may not yet have Chip & Pin cards. In order to accommodate them, you can continue to accept these cards in the normal way. Magnetic stripe cards can be accepted at Chip & Pin terminals as well, so you won't need to maintain two kinds of terminals. Simply follow the standard procedure for magnetic stripe, signature-based, or PIN transactions.

#### 5.2.10 *If a cardholder believes their PIN has been compromised*

If customers believe someone may have seen them entering their PIN, advise them to change their PIN immediately. They can do so by contacting their card issuing bank.

#### 5.2.11 *What staff training is necessary?*

Comprehensive staff training is normally required well in advance of Chip & Pin deployment. Each merchant should decide their own training needs by working with their acquiring bank.

**6. Conclusion**

It is suggested that the availability of Chip & Pin cards should be addressed in such a way that it is business as usual with a new "card" coming soon.

## Appendix A

### Glossary of Terms – Merchant Focus

- 1. Acquirer**  
The bank which recruits shops and other service providers to accept payment cards. Acquirers process a merchant's transactions and pass them into the clearing system to allow financial settlement.
- 2. Application**  
The program within a Chip & Pin card that contains processing logic which governs the Chip & Pin card's behaviour.
- 3. Authentication**  
The process of verifying that the card and/ or critical data have not been fraudulently altered or manipulated and is therefore genuine.
- 4. Authorisation**  
The process whereby a merchant (or a Cardholder through an ATM) requests permission from the Card Issuer for the card to be used for a particular transaction.
- 5. Business / Purchase Card**  
A card that is issued to businesses or companies for staff to undertake general business-related spending e.g. travel and entertainment (see also Commercial Card).
- 6. Card Acceptance Device (CAD)**  
A device used to interface with the Chip & Pin Card during a session.
- 7. Cardholder Verification Method (CVM)**  
A means of identifying that the person presenting the card is genuine. This may, for example, be performed by use of a PIN or signature in a retail outlet or by PIN at an ATM.
- 8. Cardholder**  
A person to whom a payment card has been issued.
- 9. Card Issuer**  
The bank or company which issues a Chip & Pin Card to the customer, and which has financial responsibility for a card originated transaction.
- 10. Card-Not-Present (CNP)**  
A transaction where the merchant does not have physical access to the card (e.g. through telephone, mail order or card Internet transactions).
- 11. Card Schemes/Associations**  
Banks are usually members of the appropriate scheme/association to issue cards and acquire card transactions. Examples are: Visa, MasterCard, American Express and Diners Club International.
- 12. Cardholder Activated Terminal (CAT)**  
A terminal activated by the Cardholder and not supervised by a member of staff on behalf of the merchant. May also be referred to as a Self Service Device (SSD).

**13. Charge Card (Chip & Pin)**

A Chip & Pin card, the terms of which include the obligation to settle the account in full at the end of a specified period.

**14. Chip**

An integrated circuit (e.g. for use in a Chip & Pin card).

**15. Chip & Pin Card**

A Chip & Pin card holds details on a computer chip embedded in the plastic, which can store and process information. PIN is used as the means of cardholder verification to ensure that the cardholder is legitimate and the card is not lost or stolen. It may also have a traditional magnetic stripe.

**16. Co-Branded Card (Chip & Pin)**

A Chip & Pin card issued by a bank in partnership with a non-financial institution (usually one which has a well-known brand name), bearing the brand logo of both. The non-financial institution may offer certain benefits to Cardholders, often using a points system.

**17. Commercial Card**

A generic term covering business, corporate and purchasing cards.

**18. Corporate Card**

A card which larger companies issue to staff to make business related transactions (e.g. travel and entertainment). Corporate cards often have functions other than payment.

**19. Counterfeit Card**

A card, which has been printed, embossed or encoded so as to appear to be a legitimate card.

**20. Credit Card (Chip & Pin)**

A Chip & Pin card that enables the holder to make purchases and to draw cash up to a pre-arranged limit.

**21. Cross-Border Fraud (Chip & Pin)**

Fraud perpetrated on a Chip & Pin card, or using a card number, in a country other than the country of issue.

**22. Debit Card (Chip & Pin)**

A Chip & Pin card linked to a bank account, used to pay for goods and services by debiting the holder's account, usually also combined with other facilities such as ATM functions.

**23. Electronic Purse**

A stored-value payment card that holds value which can be used for payment of goods and services. It is an alternative to cash. The card can be disposable or re-loadable, but in each case the card's stored value is reduced as payments are made.

**24. EMV**

The internationally agreed standards for chip payment cards, originally agreed by Europay, MasterCard and Visa. EMV standards are maintained by EMVCo, an organisation owned and managed by Japan Credit Bureau, MasterCard and Visa.

- 25. Fallback**

A transaction that is verified by a method other than the optimum available on both the card and the device. In a maturing Chip & Pin environment, fallback to signature, key entry or paper will be actively discouraged and will eventually disappear altogether.
- 26. Hot Card File**

A computerised list of reported lost and stolen cards, which have at least been used once fraudulently, available to merchants to assist in the identification and prevention of fraudulent transactions.
- 27. Indent printed**

Printed in such a way as to penetrate the plastic rather than just leave an image on the surface.
- 28. Loyalty Card**

Cards issued typically by retailers to earn rewards or discounts.
- 29. Magstripe**

The magnetic stripe that currently appears on the back of all payment cards issued by financial institutions. It contains essential customer and account information, most of which is usually also embossed on the card.
- 30. Merchant**

The organisation (usually a merchant: e.g. a shop, restaurant or mail order company) that accepts a card to facilitate payment.
- 31. Off-Line**

An operating mode in which the electronic terminal does not connect to a central computer source. The purchase is authorised offline without checking with the Card Issuer or their agent. The transaction is later transferred to the processing system for payment.
- 32. On-Line**

An operating mode in which the electronic terminal connects to a central computer to check Cardholder and account details with the Card Issuer, or its agent, before authorising a payment. The transaction details are transferred automatically to the processing system, either immediately or later.
- 33. Online Debit Card**

A debit card where every purchase is subject to electronic authorisation
- 34. PIN**

Personal Identification Number. A set of numeric characters, usually a four or five -digit sequence, used by the Cardholder to verify the identity at the point-of-sale or a customer activated terminal, such as an ATM. The number is generated by the Card Issuer using a secure computerised process when the card is first issued and may be changed by the Cardholder thereafter (see PIN change).
- 35. PIN Change**

The ability of a Cardholder to select a different PIN to that generated by the card issuer by whatever means.

- 36. PIN Block**  
The process by which a card is blocked from further use following a specified number of consecutive incorrect or unsuccessful PIN entries, typically three (see also PIN unblock).
- 37. PIN pad**  
The numeric pad into which a Cardholder keys their PIN to authorise a transaction. PIN pads may be fixed or portable. PIN pads are also referred to as PIN Entry Devices (PED).
- 38. PIN Services**  
The services (PIN change and PIN unlock) provided to Cardholders to enable them to manage their PINs. PIN change enables Cardholders to change the PIN to something more memorable and offers reassurance where there is concern that their PIN may have been compromised. PIN unlock ensures that Cardholders can quickly and conveniently re-establish access to card payments.
- 39. PIN Unblock**  
A process to unblock the PIN on the card. This will normally only be possible within a bank branch.
- 40. Point-Of-Sale (PoS)(or Point of Service)**  
Location where a customer makes a purchase.
- 41. PoS Terminal**  
An electronic device used to accept and process card payments at point-of-sale.
- 42. PoS Transaction**  
A transaction that takes place at a point-of-sale device.
- 43. Pre-Payment Card**  
See Electronic Purse.
- 44. Skimming**  
The most prevalent form of counterfeit fraud whereby a genuine card's magnetic stripe details are electronically copied and put onto another fake magnetic stripe card.
- 45. Self Service Device (SSD)**  
This is an unattended device through which a customer may issue payment instructions. Examples of these transactions include the drawing/ dispensing of a voucher which is redeemable for cash, making payments to third parties, making purchases and/or obtaining own account information
- 46. Type Approval**  
The terminal Type Approval process is in place to create a mechanism to test compliance with the EMV Specifications. Type Approval provides an increased level of confidence that interoperability and consistent logical behaviour between compliant applications have been achieved.